IN THE CLAIMS

Please amend the claims to read as follows:

Claims 1-31 (canceled)

32.   (Currently Amended) A system for tokenless biometric authorization of an electronic communication, using an electronic communication input apparatus, a biometric input apparatus, and a master electronic identicator, wherein said system comprises:

a.   a communication input apparatus, further comprising a data entry device for formation of an electronic communication;

b.   a biometric input apparatus connected to said communication input apparatus, further comprising a device for electronically scanning a biometric sample directly from a person of a user;

c.   at least one master electronic identicator, further comprising:

i)   a computer database containing all of the electronically stored biometric samples from all of the registered users;

ii)   a comparator that electronically compares a received biometric sample with previously stored biometric samples to deliver either a successful or failed identification of the user;

d.   a data transmittal public network that electronically transmits data between the biometric input apparatus and a master electronic identicator;

e.   an electronic communication authorization platform, connected to said master electronic identifier, that authorizes execution of at least one electronic communication upon a successful identification of the user by an electronic identicator;

f.   a rule-module clearinghouse, connected to said master electronic identifier, further comprising a user-customized rule module including at least one user-customized pattern data associated with at least one user-customized execution command, wherein said execution command comprises instructions for executing the processing of an electronic consumer loyalty or consumer rewards incentive;

g.   a rule-module invocation platform, that invokes at least one previously designated user-customized rule-module upon successful identification of the user;

h.   an electronic communication execution platform, that executes at least one electronic communication upon the invocation of a user-customized rule-module per said execution command;

wherein an electronic communication is biometrically-authorized ~~without the user having to present smartcards or magnetic stripe cards~~ in a tokenless manner.

33.   (Original)   The device of claim 32 wherein the master electronic identicator further comprises a computer database which: has a location which is physically remote from the site at which the user submits a biometric sample directly from his person, and; requires the use of a public communication network that enables receipt of an electronically transmitted registration biometric sample.

34.   (Original)   The device of claim 32 further comprising a subset electronic identicator having: a computer database containing a subset of all stored biometric samples from registered users in the computer system, and; a comparator that compares a received biometric sample with previously stored biometric samples to deliver either a successful or failed identification of the user.

35.   (Original)   The device of claim 32 wherein any component of said system is used in any of the following chronological sequences: simultaneously, and; separated by any increment of time including seconds, minutes, hours, days, weeks, months, and years.

36.   (Previously presented)   The device of claim 34, further comprising a data transmittal public network, comprising a public communications network that electronically transmits data between the subset electronic identicator and a master electronic identicator if the comparator of the subset electronic identicator returns a failed identification result.

37.   (Previously Presented)   The device of claim 34 further comprising:

a.   an enterprise data input apparatus for an enterprise to electronically input registration identity data;

b. a data transmittal public network, further comprising a public communications network that electronically transmits data between the enterprise data input apparatus and a master electronic identicator;

c. an electronic communication authorization platform, that authorizes execution of an electronic communication upon a successful identification of the enterprise by an electronic identicator and a successful identification of the user by an electronic identicator;

wherein an electronic communication is biometrically-authorized without the user having to present smartcards or magnetic swipe cards.

38. (Original) The device of claim 37 wherein any component is used in any of the following chronological sequences: simultaneously, and; separated by any increment of time including seconds, minutes, hours, days, weeks, months, and years.

39. (Previously presented) The device of claim 37, further comprising a data transmittal public network, further comprising a public communications network that electronically transmits data between the subset electronic identicator and a master electronic identicator if the comparator of the subset electronic identicator returns a failed identification result.

40. (Original) The device of claim 32 wherein the biometric sample taken directly from the person of the user comprises any of the following: a fingerprint, a facial scan, a retinal image, an iris scan, and a voice print.

41. (Original) The device of claim 37 wherein the enterprise is a legally formed entity comprising any of the following: a corporation, a foundation, a non-profit organization, a sole proprietorship, a limited liability company, and a partnership.

42. (Original) The device of claim 32 wherein the user further provides a personal identification code to the electronic identicator along with a bid biometric sample for purposes of identifying the user.

43. (Original) The device of claim 37 further comprising a user re-registration platform, wherein the user's registration biometric sample is compared by at least one electronic identicator to previously registered biometric samples wherein if a match occurs, the electronic identicator is alerted to the fact that the user has attempted to re-register.

44. (Original) The device of claim 42 further comprising a biometric theft resolution platform, wherein a user's personal identification code is changed when the user's registered biometric sample is determined to have been fraudulently duplicated.

45. (Original) The device of claim 32, wherein an electronic communication comprises any of the following: an email, a telephone call, an encrypted data packet, an Internet telephony, and a facsimile.

46. (Original) The device of claim 32, wherein the data transmittal public network further comprises any of the following: an extranet, a wide area network, a cable network, a wireless network, a telephone network, the Internet, an ATM network, or an X.25.

47. (Original) The device of claim 37 wherein enterprise registration identity data comprises any of the following: an alpha-numeric code, a hardware identification code, an email address, a financial account, a biometric of an authorized enterprise representative, a non-financial data repository account, a telephone number, a mailing address, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, and an instant messaging address.

48. (Original) The device of claim 32 further comprising a third-party server interconnecting network, wherein the electronic communication execution platform interconnects with one or more third-party servers in order to execute the electronic communication.

49. (Canceled)

50.   (Previously presented)   The device of claim 32 wherein pattern data comprises any of the following: demographic information; an email address; a financial account; internet browsing patterns; a non-financial data repository account; a telephone number; a mailing address; purchasing patterns; database authorization fields; financial credit report data; a call-center queuing, routing and automated response program; an email-center queuing, routing and automated response program; data on pre-paid accounts or memberships for products or services; electronic data utilization patterns; employee status; job title; data on user behavior patterns; a digital certificate; a network credential; an internet protocol address; a digital signature; an encryption key; an instant messaging address; user-customized medical records; an electronic audio signature; and an electronic visual signature.

51.   (Previously presented)   The device of claim 32 wherein said execution commands further comprise user-customized instructions for execution of any of the following: accessing of stored electronic data, processing of electronic data, and presentation of electronic data.

52.   (Original)   The device of claim 51 wherein user-customized accessing of stored electronic data further comprises execution of any of the following: activation of an Internet-connected device; accessing of a secured physical space, and unlocking of a secured physical device.

53.   (Previously Presented)   The device of claim 51, wherein user-customized processing of electronic data further comprises invoking any of the following: a digital certificate, an identity scrambler, a database authorization field, an electronic advertisement, an instant messaging program, real-time tracking of an incoming caller or an email sender, a time and attendance monitoring program, an emergency home alarm and personal safety notification program, a real-time challenge-response program, a call-center queuing prioritization program, a call-center routing prioritization program, an email-center queuing prioritization program, an email-center routing prioritization program, an automated caller or emailer response program, a call-forwarding program, and an electronic intelligent software program for electronic data search and retrieval.

54. (Original) The device of claim 51 wherein user-customized presentation of electronic data comprises any of the following: a print-out, a computer screen display, an audio message, a tactile sensation and a holographic image.

55. (Previously presented) The device of claim 32 wherein the rule-module invocation platform is interconnected with one or more third-party computers.

56. (Previously presented) The device of claim 32, wherein user-customized pattern data is provided to the electronic rule-module clearinghouse by any of the following: the user, the electronic identicator, the electronic rule-module clearinghouse, and a user-authorized third party.

57. (Canceled)

58. (Previously presented) The device of claim 32, wherein:
the rule-module clearinghouse includes a master rule-module clearinghouse, comprising a computer database storing all of the rule-modules for all of the registered users; and
the device further comprises a subset rule-module clearinghouse, comprising a computer database storing a subset of all of the rule-modules for registered users.

59. (Original) The device of claim 32 wherein the data transmittal public network further comprises: a cable network, a wireless cellular network, a wireless digital network, a telephone network, a wide area network, the Internet, an ATM network, and an X.25 connection.

60. (Previously Presented) The device of claim 32 wherein the master electronic identicator further comprises a computer database having a location which is physically remote from the site at which the user submitted the registration biometric sample.

61. (Previously Presented) The device of claim 34 wherein the subset electronic identicator further comprises a computer database: being physically remote from the

master identicator, and; capable of using any communications network for receiving the bid biometric sample.

62.   (Previously Presented)   The device of claim 58 further comprising:

a first rule-module invocation platform, comprising a subset rule-module clearinghouse that invokes at least one user-customized rule-module;

a data transmittal public network, wherein if the subset rule-module clearinghouse fails to invoke a user-customized rule-module, the request is transmitted via a public communications network to a master rule-module clearinghouse;

a second rule-module invocation platform, comprising a master rule-module clearinghouse that invokes at least one user-customized rule-module;

an electronic communication execution platform, that executes at least one electronic communication upon the earliest invocation of a user-customized rule-module by a rule-module clearinghouse.

63.   (Previously Presented)   The device of claim 58 wherein the subset rule-module clearinghouse is physically remote from the master rule-module clearinghouse.

64.   (Canceled)

65.   (Previously presented)   The device of claim 53 wherein pattern data comprises any of the following: demographic information; an email address; a financial account; internet browsing patterns; a non-financial data repository account; a telephone number; a mailing address; purchasing patterns; database authorization fields; financial credit report data; a call-center queuing, routing and automated response program; an email-center queuing, routing and automated response program; data on pre-paid accounts or memberships for products or services; electronic data utilization patterns; employee status; job title; data on user behavior patterns; a digital certificate; a network credential; an internet protocol address; a digital signature; an encryption key; an instant messaging address; user-customized medical records; an electronic audio signature; and an electronic visual signature.

66.   (Canceled)

67.   (Previously Presented)   The device of claim 32 wherein:

the system further comprises means for receiving a personal identification code coupled to the biometric input apparatus;

the computer database contains all of the electronically stored biometric samples and associated personal identification codes from all of the registered users; and

the comparator electronically compares the received biometric sample with previously stored biometric samples associated with the personal identification code to deliver either a successful or failed identification of the user.

68.   (Canceled)

69.   (Canceled)